UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/830,685	07/17/2001	Christophe Clavier	032326-138	9929

32291 7590 01/06/2005

MARTINE PENILLA & GENCARELLA, LLP
710 LAKEWAY DRIVE
SUITE 200
SUNNYVALE, CA 94085

EXAMINER	
ABYANEH, ALI S	
ART UNIT	**PAPER NUMBER**
2133	

DATE MAILED: 01/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/830,685	CLAVIER ET AL.	
	Examiner	Art Unit	
	Ali S. Abyaneh	2133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 7/17/01

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-8,11-15 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-8 and 11-15 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner for the Abstract is missing. 42

10)☒ The drawing(s) filed on 7/17/01 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 4/30/01.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the applicant's preliminary amendment dated 04/30/2001. In the amendment claims 9 and 10 were canceled and new claims 11-15 were added. Therefor, claims 1-8 and 11-15 remains pending in the application.

2. Claims 1-15 have been examined.

3. Foreign Priority benefit claimed under Title 35, United States Code, § 119 have been acknowledged.

Information Disclosure Statement PTO-1449

4. The Information Disclosure Statement submitted by applicant on 04/30/2001 (paper number 3) has been considered. Please see attached PTO-1449.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Regarding claim 1

The term "critical instruction" in claim 1 is a relative term which renders the claim indefinite. The term " critical instruction " is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

(Examiner interprets critical instructions as permutations).

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claim 1,6-15 are rejected under 35 U.S.C. 102(e) as being anticipated by Paul c. Kocher (US Patent NO. 6,278,783) .

Regarding claim 1

Kocher explicitly teaches a countermeasure method in an electronic component using a cryptographic algorithm with a secret key, (column 12, lines

18-24) which algorithm utilizes a first manipulating means for supplying an output data item from an input data item, (column 6, lines 39-42) and the output data item manipulated by means of critical instructions, [(Examiner interprets critical instruction as permutation)(column 6, lines 47-49)] said method including the step of utilizing other manipulation means for supplying output data, so that the output data item is unpredictable, said other means being obtained from said first manipulation means by an exclusive OR operation with a random value. (column 6, lines 39-53, where the output data is unpredictable (random)).

Regarding claim 6

Kocher teaches a countermeasure method according to claim 1 wherein each execution of the algorithm includes the steps of drawing a random value and calculating said other manipulation means. (column 6, Lines 39-53).

Regarding Claim 7

Kocher teaches a method according to claim 1 wherein said manipulation means are tables of constants. (column 7, Lines 16-65).

Regarding claim 8

Kocher teaches a method according to claim 1 wherein said manipulation means are used in combination with an additional exclusive OR operation with a value based upon the random value. (column 6, lines 39-53).

Regarding Claim 11

Kocher teaches the method of claim 1 wherein said random value is derived from one or both of the input and output data of said first manipulation

means. (column 6, Lines 39-53).

Regarding claim 12

Kocher teaches an electronic security component have a countermeasure against attacks on a secret key cryptography technique in which data is manipulated by critical instructions, said component comprising: a program memory having stored therein a first manipulating means for use during said critical instructions; (column 2, lines 35,36) means for generating a random value, and means for calculating at least one other manipulating means from said random value, to be employed during a given execution of said cryptography technique. (column 6, lines 39-53).

Regarding claim 13

Kocher teaches the electronic security component of claim 12, wherein said first and said other manipulating means each comprise a table of constants. (column 7, lines 16-65).

Regarding claim 14

Kocher teaches the electronic security component of claim 12, wherein Said cryptography technique comprises a DES algorithm that is executed in multiple rounds. (column 9, lines 1-67, column 10, lines 1-39 and column 11, lines 41-55).

Regarding claim 15

Kocher teaches the electronic security component of claim 12, wherein said component is a chip card. (column 14, lines 1-8).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) patent may not be obtained though the invention is not identically disclose or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 2 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher (US Patent NO.6278783).

Regarding claim 2 and claim 5

Kocher teaches a method according to Claim 1, wherein said algorithm comprises sixteen calculation rounds, each round using manipulation means for supplying an output data item from an input data item, (column 9, lines 1-67, column 10, line 1-38 and Fig 1). However, Kocher does not explicitly teach the output data item being manipulated and executed by critical instructions in the first three and the last three rounds, and wherein said method includes the steps of forming a first group comprising at least the first three rounds and another group comprising at least the last three rounds. Kocher, however does teach the manipulation and execution could be done at the beginning or at the end of DES (Data Encryption Standard) operation. (see column 9, lines 14-17). This would have been obvious to one of ordinary skill in the art at the time the invention was made, since Kocher teaches implementation and execution at the

beginning or at the end of DES operation. Therefore one ordinary skill in the art at the time the invention was made would have been motivated to utilize manipulation and execution from the beginning and the end as thought by kocher in order to improve implementation of the DES, and associating with the first group and with the last group an execution sequence using the other manipulation means in at least some rounds. (column 9, lines 1-67, column 10, lines 1-38 and Fig 1).

10. Claims 3 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher (US Patent NO.6278783) in view of Luyster (US Patent NO 6182216).

Regarding claim 3 and claim 4

Kocher teaches a countermeasure method according to Claim 2, Kocher does not explicitly teach four groups of successive rounds and applying the execution sequence at least to the first group and to the last group, wherein the sequence is executed in each of the groups. However Luyster, in an analogous art, teaches four groups each of four successive rounds are formed, and said execution sequence is applied at least to the first group and to the last group, wherein the sequence is executed in each of the groups. (see column 7, lines 16-51). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method of multiple rounds operations disclosed by Kocher to form four groups each of four successive rounds, and apply said execution sequence to the first group and the

last group, and furthermore execute the said sequence in each of the groups, as thought by Luyster. This would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do this modification since applying more instructions and rounds to DES operation would make the encryption more complex and more random . Therefore this modification would lead to a grater security level.

References Cited, Not Used

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

1. U.S.Patent No.6,490,357

This reference relates to a method and apparatus for generating encryption stream ciphers.

2. U.S.Patent No. 5,675,649

This reference teaches a process and a system for cryptographic key generation and safekeeping.

3. U.S.Patent No. 6,282,291

This reference relates to an encrypting method and apparatus for encrypting a key employed for encryption and outputting it in the form of text.

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ali Abyaneh whose telephone number is (571) 272-7961. The examiner can normally be reached on Monday-Friday from (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on (571)272-3819. The fax phone numbers for the organization where this application or proceeding is assigned as (703) 872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Gay J. LAMARRE
PRIMARY EXAMINER

Ali Abyaneh
Patent Examiner
Art Unit 2133

Dec 22, 2004

A. A